JOURNAL OF NUMBER THEORY 3, 210–212 (1971)

Proof of a Conjecture of S. Chowla

RIMHAK REE

Department of Mathematics, University of British Columbia, Vancouver 8, Canada

Communicated by S. Chowla

Received February 11, 1970

A conjecture of Chowla on the number of integers a between 1 and $p-1$ for which the polynomial $x^n + x + a$ becomes irreducible (mod p) is proved. The same arguments show that $x^n + x + a$ can be replaced by more general polynomials.

The conjecture mentioned in the title is the following: *For every* $n \geqslant 2$, *the number of polynomials*

$$x^n + x + a \; (1 \leqslant a \leqslant p-1),$$

which are irreducible (mod p), *is asymptotic to* p/n *as the prime* p *tends to* ∞.

The case $n = 3$ was proved by Chowla [2] himself, and the case $n = 4$ has recently been proved by K. S. Williams [7] and P. A. Leonard [5].

In this note we shall show that the truth of the conjecture is an immediate consequence of a density theorem of Weil [6, 4] and the fact, proved by Birch and Swinnerton-Dyer [1], that the Galois group of the polynomial $x^n + x + t$ over the field $\bar{F}_p(t)$ of rational functions in the variable t, where $\bar{F}_p$ is an algebraic closure of the prime field F_p of p elements, is the symmetric group S_n, provided $p \nmid 2n(n-1)$.

Let k be a finite field of q elements and of characteristic p. Let $k(t)$ be the field of rational functions in the variable t over k, and let K be the splitting field of the polynomial $f(x) = x^n + x + t$ over $k(t)$. Denote by D the set of elements a in k such that the place $\mathfrak{p}_a$ of $k(t)$ corresponding to $t - a$ does not ramify in K. For each $a \in D$ and each place $\mathfrak{P}$ of K lying above $\mathfrak{p}_a$ denote by $\sigma_{\mathfrak{P}}$ the Frobenius generator of the decomposition group of $\mathfrak{P}$. When $\mathfrak{P}$ runs over all places in K lying over $\mathfrak{p}_a$, $\sigma_{\mathfrak{P}}$ fills up a conjugacy class of the Galois group G of $K/k(t)$, which we shall denote by C_a. For any conjugacy class C in G, let $N_n(C)$ be the number of ele-

ments $a \in D$ such that $C_a = C$. Then the density theorem of Weil [6, 4] says that there exist a constant A_n, depending only on n, such that

$$\left| N_n(C) - \frac{|C|}{|G|} q \right| < A_n q^{1/2}, \tag{1}$$

where $|S|$ denotes the cardinality of the finite set S. The fact that the constant A_n depends only on n follows from the fact that the genus of the field K is a constant, depending only on n, for sufficiently large p.

Let $L/k(t)$ be a separable extension contained in $K/k(t)$, corresponding to a subgroup H of G. For any $a \in D$, let $\mathfrak{P}$ be a place of K lying above $\mathfrak{p}_a$ and let Z be the decomposition group of $\mathfrak{P}$. Then Z is a cyclic group generated by the Frobenius automorphism $\sigma_{\mathfrak{P}}$, and there is a one-to-one correspondence between the places $\mathfrak{p}_i$ in L lying above $\mathfrak{p}_a$ and the double cosets $Z\sigma_i H$ of (Z, H) in G; moreover, the number of left cosets of H contained in $Z\sigma_i H$ is equal to the degree of $\mathfrak{p}_i$. In particular, there is only one place in L above $\mathfrak{p}_a$ if and only if $G = ZH$.

Let $L/k(t)$ be the subfield of $K/k(t)$ obtained by adjoining only one root θ of $f(x) = 0$, and regard G as a permutation group of the roots $\theta, \theta', \ldots$ of $f(x) = 0$. Then the subgroup H corresponding to L consists of the elements in G fixing θ. Now assume that $t = a$ is not a root of the discriminant $\pm(n^n t^{n-1} + (1 - n)^{n-1})$ of $f(x)$. Then $a \in D$, and there is a one-to-one correspondence between the places of L lying above $\mathfrak{p}_a$ and the (monic) irreducible factors of $x^n + x + a$ over k, where the degree of the place and that of the corresponding irreducible factor coincide. In particular, $x^n + x + a$ is irreducible over k if and only if $G = ZH$, where Z is the decomposition group of an (arbitrary) place in K lying above p_a.

By Birch and Swinnerton-Dyer [1], $G = S_n$ if $p \nmid 2n(n-1)$. In this case, let Z be a cyclic subgroup of order n of G such that $G = ZH$, and let σ be a generator of Z. Let $\sigma = \sigma_1\sigma_2 \cdots$ be the decomposition of σ into a product of disjoint cyclic permutations and let σ_1 be the one that moves the root θ. Let m be the order of σ_1. Then $\sigma^m \in H$ and hence $m = n$, $\sigma = \sigma_1$. Thus σ is a cyclic permutation of order n. There are $(n-1)!$ cyclic permutations of order n and they form a single conjugacy class C.

Denote by $N_n(q)$ the number of elements $a \in k$ for which $x^n + x + a$ is irreducible over k. Then clearly $0 \leqslant N_n(q) - N_n(C) \leqslant n - 1$, and $|C|/|G| = 1/n$. Hence from (1) one gets the following:

THEOREM 1. *Assume that $p \nmid 2n(n-1)$. For each $n \geqslant 2$, there exist a constant B_n, depending only on n, such that*

$$\left| N_n(q) - \frac{q}{n} \right| \leqslant B_n q^{1/2}.$$

The polynomial $x^n + x + t$ can be replaced by any irreducible polynomial $f(x)$ in $k(t)[x]$ as long as one knows its Galois group over $k(t)$, and the same arguments go through. See [1] and [3] for other polynomials whose Galois groups are known to be symmetric or alternative.

If the degree n of $f(x)$ is a prime, there is always a cyclic group Z of order n such that $G = ZH$, since the order of G is divisible by n while the order of H is not. From this one can deduce the following

THEOREM 2. *Let n be a prime, and let*

$$f_t(x) = a_0(t)\, x^n + a_1(t)\, x^{n-1} + \cdots + a_n(t)$$

be a polynomial of degree n with coefficients in $\mathbf{Z}[t]$ which is irreducible in $\mathbf{Q}(t)[x]$. Then there are three constants p_0, B, and $\lambda > 0$, all depending on $f_t(x)$, such that for $p > p_0$

$$| N(q) - \lambda q | < Bq^{1/2},$$

where $N(q)$ denotes the number of elements $a \in F_q$, where F_q is a finite field of q elements of characteristic p, such that $f_a(x)$ remains irreducible of degree n over F_q.

ACKNOWLEDGMENT

I would like to thank Klaus Hoechsmann for the conversations I had with him while preparing this note.

REFERENCES

1. B. J. BIRCH AND H. P. F. SWINNERTON-DYER, Note on a problem of Chowla, *Acta Arith.* **5** (1959), 417–423.
2. S. CHOWLA, A note on the construction of finite Galois fields $GF(p^n)$, *J. Math. Anal. Appl.* **15** (1966), 53–54.
3. D. HILBERT, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *J. Angew. Math.* **110** (1892), 104–129.
4. S. LANG, Sur les séries L d'une variété algébrique, *Bull. Soc. Math. France* **84** (1956), 385–407.
5. P. A. LEONARD, On constructing quartic extensions of $GF(p)$, *Norske Vid. Selsk. Forh. (Trondheim)* **40** (1967), 96–97.
6. A. WEIL, "Sur les courbes algébriques et les variétés qui s'en déduisent," Hermann Paris, 1948.
7. K. S. WILLIAMS, On two conjectures of Chowla, *Canad. Math. Bull.* **12** (1969), 545–565.